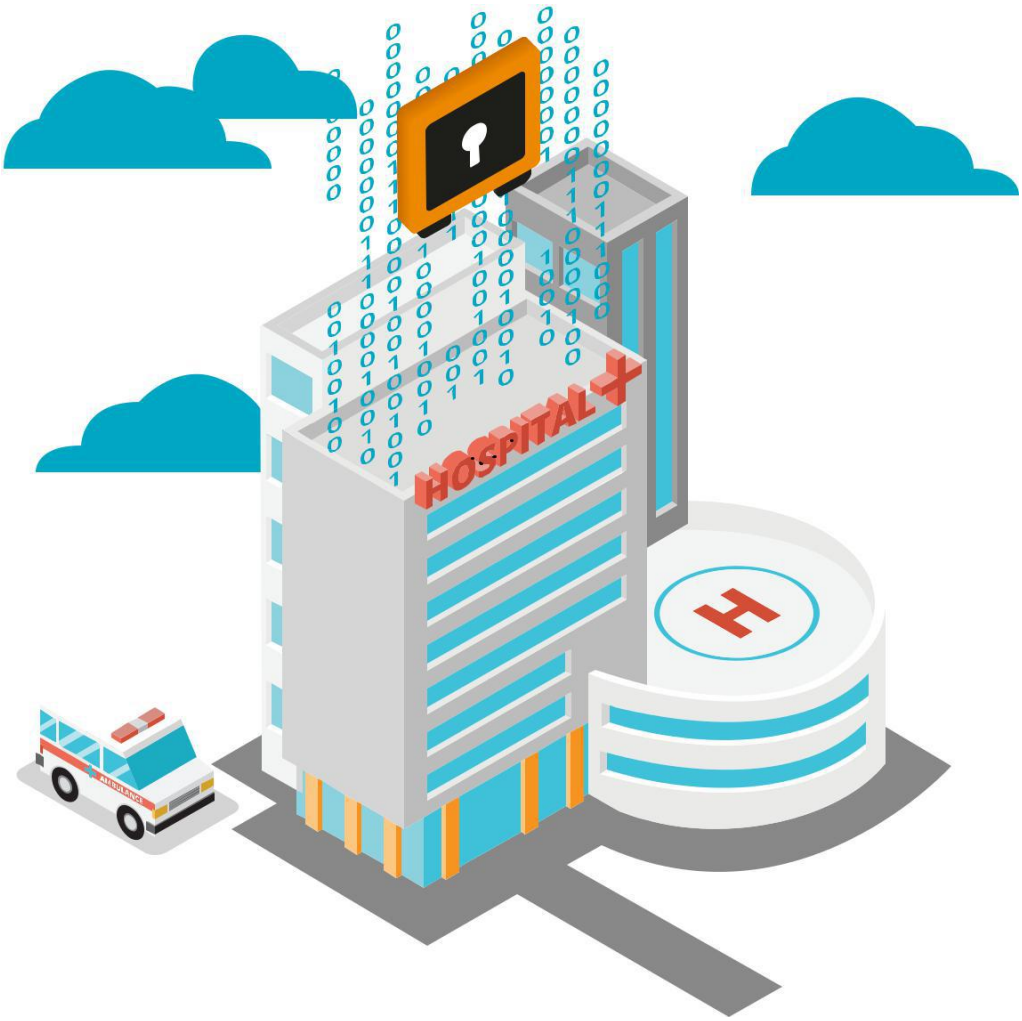
KeepItSafe®
ONLINE BACKUP

WHAT YOU NEED TO KNOW ABOUT

HIPAA AND ONLINE BACKUP



www.keepitsafe.com

TABLE OF CONTENTS

WHAT YOU NEED TO KNOW ABOUT HIPAA AND ONLINE BACKUP

Whether you're a healthcare provider, health plan or a non-healthcare business that deals with patients' private medical data — called electronic protected health information, or ePHI — your company falls under the complex and aggressively enforced federal HIPAA law. And if even you've already taken steps to safeguard this sensitive data when your staff transmits it, you must keep in mind that HIPAA also places strict requirements on how you store and back up any ePHI under your care.

Understanding these backup requirements, and deploying the right solution to back up your ePHI, can help keep you on the right side of HIPAA's enforcers, save you from the law's steep fines for violations, and even prevent the public damage your business's reputation can suffer as the result of just one mistake.

A HEALTH-DATA BACKUP HORROR STORY

When he placed a set of his company's backup tapes in his car for transport, the employee of Science Applications International Corp. (SAIC) had no idea that this routine action would lead to the largest breach of patient health data ever reported by the Department of Health and Human Services. Nor could he know then that this simple mistake would expose his company to a nearly $5 billion class-action lawsuit from the millions of patients it affected.

But those backup tapes — which contained unencrypted ePHI under the care of SAIC, a subcontractor for the US military's health system TRICARE — were stolen from the employee's car. The breach affected all of those TRICARE patients who received treatment at a specific medical facility in the decade between 1992 and 2011 — a total of 4.9 million active and retired personnel and their family members.

LESSONS FROM THIS HORROR STORY

The number of missteps in the true story above is greater than it might seem at first. So before we delve into a discussion of HIPAA and its strict guidelines governing the backup of electronic protected health information, here's a quick recap of where SAIC (and TRICARE) ran afoul of HIPAA:

1. **The Ability to Meet Recovery Time Objectives (RTOs)**

   HIPAA's Security Rule (45 C.F.R 164.306, in case you're wondering), requires a "Covered Entity" or "Business Associate" establish "physical measures, policies and procedures" to protect the business's "electronic information systems and related buildings and equipment" from, among other things, "unauthorized intrusion."

   Clearly, allowing patient ePHI to be stored on backup tapes that are then carried to an employee's car fall short of this requirement.

2. **They failed to comply with encryption requirements.**

   Remember, the ePHI on the stolen backup tapes was also unencrypted, in violation of section 13402(h) of the HITECH Act, a 2009 expansion to federal healthcare law.

   This section demands that ePHI must be either "encrypted or destroyed" to ensure its security at all times.

3. **They took too long to notify those patients affected.**

   Another component of HIPAA compliance involves the Covered Entity's breach-notification procedures. The HIPAA Notification Rule (45 C.F.R. 164.400-414, in case you're wondering) requires "Covered Entities and their Business Associates to provide notification following a breach of unsecured protected health information."

   The notification requirements are deadline-specific and wide-reaching: Covered Entities must notify affected individuals within 90 days of a breach, for example, provide media notification within 60 days, and notify the HHS Secretary within 60 days. The SAIC-TRICARE lawsuit argued the businesses did not meet these deadlines.

4. **They failed to meet their shared responsibility as a BA.**

   Finally, it's worth pointing out that as a subcontractor to the military's health system TRICARE, SAIC was acting as a Business Associate — defined as a third party working with a HIPAA Covered Entity (in this case, TRICARE), which deals with ePHI on behalf of that Covered Entity as part of its business relationship.

   SAIC was collecting and storing ePHI as a TRICARE contractor, and as a result, they had a shared responsibility to protect that patient data. As a result of this failure to properly back up the ePHI under their charge, SAIC exposed both itself and TRICARE to HIPAA regulators and the class-action lawsuit that followed.

BACKGROUND:
WHAT IS HIPAA?

Passed by Congress in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a federal law enacted to protect the security and confidentiality of patients' personal medical data — called protected health information, or PHI. Here is a brief list of the specific objectives of the HIPAA law in it original format:

1. To increase the security and portability of patient records
2. To provide the ability to securely and easily transfer a patient's health insurance seamlessly from one plan to another
3. To reduce health fraud and abuse
4. To establish mandated, industry-wide standards for electronic billing of medical records
5. To require the protection and confidential handling of protected health information (PHI), whether in hardcopy or electronic formats

HIPAA enforcement has continually strengthened since its passage 20 years ago, and the law itself has expanded in scope. The HITECH Act was enacted in 2009, for example, to give federal regulators more authority to address the rapidly expanding use of electronically based protected health information (ePHI).

Then in 2013, HHS published its Final Omnibus Rule, which expanded regulators' oversight of patient information — to include any vendor (called a "Business Associate") that creates, receives, maintains or transmits PHI on behalf of Covered Entity such as a healthcare provider or health plan.

WHAT CONSTITUTES PHI?

Protected health information (PHI) refers to any personally identifiable data relating to the physical or mental health of an individual, the provision of healthcare services for that individual, or the payment for healthcare services on behalf of an individual. These pieces of data could include:

- Patient name
- Patient address
- Patient birthdate
- Patient Social Security Number
- Medical records
- Medical billing details
- Any other information that can be used to identify a specific person

This is why HIPAA's oversight reaches well beyond healthcare providers and health plans — clearly, many third parties that play an integral role in patient health also handle ePHI.

In other words, if you're wondering whether your organization falls under HIPAA's oversight and enforcement, it probably does. To be sure, though, let's review the wide range of entities that share responsibility — as Covered Entities (CEs) or Business Associates (BAs) — for protecting patients' protected health information.

WHO IS RESPONSIBLE FOR SAFEGUARDING PHI?

Businesses with regulatory responsibility for safeguarding the ePHI they deal with fall under two categories: Covered Entities and Business Associates:

Covered Entities (CEs)

Healthcare Providers: Doctors, clinics, hospitals, pharmacies, psychologists, nursing homes and dentists — any healthcare entity that deals with ePHI.

Health Plans: Health insurers, HMOs, company health plans and certain government entities that pay for healthcare, such as Medicare and Medicaid.

Healthcare Clearinghouses: Entities that process nonstandard health information from another entity into standard format (for example, into an electronic form.)

Business Associates (BAs)

This would include all of the non-healthcare businesses — contractors, subcontractors or third-party vendors — working with Covered Entities that must handle, store or transmit ePHI as part of their standard business practices.

Like the CEs they work with, these BAs share the responsibility for the security of the ePHI under their charge, and as a result they're regulated by HIPAA.

Examples of BAs include medical billing companies, businesses that administer health plans, lawyers, accountants, IT consultants, and businesses that store, back up or destroy patient records for CEs.

KeepItSafe would qualify as a Business Associate — because we securely backup ePHI for our healthcare customers. And we sign a Business Associate Agreement (BAA) as part of our standard practice when helping a HIPAA-regulated healthcare business back up its patient data.

Remember: The 2013 Final Omnibus Rule, published by the HHS, expanded the Privacy Rule's definition of a Business Associate to include any vendors that "create, receive, maintain or transmit" PHI on behalf of a Covered Entity.

THE HIGH COST OF A HIPAA VIOLATION

To give you an idea of the monetary costs of making just a single mistake in terms of how a Covered Entity or its Business Association, have a look at the table below, published by the American Medical Association and addressing failure to comply with HIPAA (Section 42 USC 1320d-5):

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Source: *American Medical Association.*

A single HIPAA violation can cost a Covered Entity $50,000 per occurrence —and in cases where each occurrence impacts many people, that per-occurrence penalty can reach $1.5 million in fines annually.

A Costly HIPAA Backup Violation

Consider this real-world example of how a mishandling of ePHI backup can lead to a huge fine — not to mention the negative publicity of reports about your patients' private medical data being stolen.

In 2010, Massachusetts-based South Shore Hospital shipped three boxes of backup tapes (nearly 500 tapes in all) to Archive Data Solutions, to have the tapes wiped clean of their data — unencrypted ePHI on 800,000 patients.

Turns out only one of the three boxes made it to Archive Data Solutions. The other two, containing hundreds of thousands of unencrypted patient records, went missing. According to the Massachusetts Attorney General, South Shore Hospital failed to securely back up its ePHI, failed to inform Archive Data Solutions about the sensitive nature of the data it was receiving, failed to put in place a Business Associate Agreement (BAA) with Archive Data, and failed to determine first whether or not Archive Data had the proper safeguards in place at its facilities before shipping ePHI to the company.

All told, South Shore Hospital paid $750,000 in fines for these HIPAA violations.

Another Costly HIPAA Violation

In 2013, Illinois-based Advocate Medical Group suffered a break-in at its facility and thieves took off with four laptop computers containing the Social Security numbers and other ePHI of more than four million people. This qualified at the time as second-largest health-related data breach ever.

According to the lawsuit filed by affected patients against the healthcare organization, Advocate Medical's laptops were unencrypted and stolen from an unmonitored room with "little or no security to prevent unauthorized access."

Note: The security and HIPAA-violation implications of this laptop-theft incident underscore the need for any Covered Entity or Business Associate to deploy a companywide solution for Mobile Device Management, such as the one available from **KeepItSafe Mobile.**

STILL NOT CONVINCED YOU NEED A BACKUP SOLUTION THAT ADDRESSES HIPAA?

Perhaps you need further convincing that your company's data backup solution must take HIPAA's regulations into account, assuming you ever deal directly with PHI. If so, please read the excerpts below from an article published by the Healthcare Billing & Management Association — a 30-year trade association whose members today are responsible for nearly 80% of all third-party medical-billing claims in the country.

In its feature, "**The Truth About HIPAA-HITECH and Data Backup**," the association warns its medical-billing members (all BAs, regulated by HIPAA):

- It's not optional - All CEs, including medical practices and BAs, must securely back up "retrievable exact copies of electronic protected health information" (CFR 164.308(7)(ii) (A)).
- Your data must be recoverable - Why else are you backing it up? You must be able to fully "restore any loss of data" (CFR 164.308(7)(ii).
- You must get your data offsite - as required by the HIPAA Security Final Rule (CFR 164.308(a)(1)). How could one defend a data backup and disaster recovery plan that stored backup copies of ePHI in the same location as the original data store?
- You must back up your data frequently - as required by the HIPAA Security Final Rule (CFR 164.308(a)(1)). In today's real-time transactional world, a server crash, database corruption, or erasure of data by a disgruntled employee at 4:40 PM would result in a significant data loss event if one had to recover from yesterday's data backup.

Finally, the piece points out:

- Non-compliance penalties are severe - Penalties are increased significantly in the new tiered Civil Monetary Penalty (CMP) System with a maximum penalty of $1.5 million for all violations of an identical provision."

HOW TO FIND A HIPAA-COMPLIANT DATA BACKUP SOLUTION

Many online backup provider claim their processes meet HIPAA standards. And when it comes to certain guidelines and clauses, they might be. But be careful — the HIPAA Security Rule demands that a Covered Entity have a backup plan that meets all of HIPAA's criteria.

When choosing a data backup solution that will protect your ePHI and meet HIPAA's requirements, you will need to judge that solution against HIPAA's mandates regarding:

1. **Offsite Data Backup**
   You'll need your backup stored offsite, at physical locations other than your primary facilities. (45 C.F.R. 164.308)

2. **Encryption**
   You'll need to keep your at-rest ePHI data encrypted at all times — or destroy it — to ensure its security. (Section 13402(h) of Title XIII of the HITECH Act)

3. **Technical Safeguards**
   You'll need to employ sufficient technology, and the policies and procedures for its use, to protect your ePHI and control access to it. (45 C.F.R. 164.306)

4. **Physical Safeguards**
   You'll need to implement physical measures, policies and procedures to protect your electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion. (45 C.F.R. 164.306)

5. **Administrative Safeguards**
   You'll need to implement policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of your workforce in relation to the protection of that information. (45 C.F.R. 164.306)

6. **Business Associate Agreement**
For any Business Associate you work with that will need to access or maintain your ePHI — and an online backup service qualifies — you will need that entity to sign a Business Associate Agreement (BAA), which places the BA under shared responsibility with you for all ePHI they handle, in accordance with HIPAA guidelines. (45 C.F.R. 160.103)

Note: You should immediately dismiss from consideration any would-be online backup provider that refuses to sign a binding BAA with you.

HIPAA Requirement	Clause	keepitsafe
Backup All Covered entities and business associates must securely back up "retrievable exact copies of electronic protected health information"	(CFR 164.308(7)(ii) (A)).	**We back up exact copies of your all of your data — emails, SQL files, meta data, etc.**
Recovery You must be able to fully "restore any loss of data"	(CFR 164.308(7)(ii) (B)).	**Our suite of backup and DR solutions allows for the total restore of any lost data — and we have the success stories to prove it.**
Offsite Data Backup You must store your data offsite	(CFR 164.308(a)(1)) - HIPAA Security Final Rule	**We provide cloud and hybrid-based backup, protecting your ePHI multiple, geographically redundant, tier-4 data centers.**
Encryption/ Data Destruction ePHI must be encrypted or destroyed at rest to secure it.	Section 13402(h) of Title XIII HITECH Act	**We provide military-grade, 256-bit encryption (FIPS -140-2) — and ensure only you have an encryption key, to comply with the Privacy Law.**
Testing "Implement procedures for periodic testing and revision of contingency plans."	(CFR 164.308(7)(ii) (D)).	**KeepItSafe DR includes regular testing to ensure ongoing ePHI security and your compliance with HIPAA.**

HIPAA Requirement	Clause	keepitsafe
Technical Safeguards Technology and the policy and procedures for its use that protect electronic protected health information and control access to it.	45 C.F.R. §164.306 (Security Rule)	**ISO-27001 Suite of Data Recovery Solutions Fully Managed and Monitored Encryption.**
Physical Safeguards Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic **information systems** and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.	45 C.F.R. §164.306 (Security Rule)	**KeepItSafe protects your ePHI at all times in state -of-the-art secure data centers — protected by firewalls, onsite guards 24/7 and biometric and other physical restrictions.**
Administrative Safeguards Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of **security measures** to protect ePHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.	45 C.F.R. §164.306 (Security Rule)	**We deploy protective data safeguards designed specifically for ePHI — and we offer third-party employee training to ensure a security and compliance culture.**
The Privacy Rule 40 pages, but includes patient confidentiality and business associates agreements	45 C.F.R. §160.103	**KeepItSafe will enter into a BAA for contractual assurance that your ePHI security complies with HIPAA.**
Disaster Recovery Planning The Covered Entity or Business Associate must maintain readiness for lost ePHI.	Federal Register Vol 68, no 34, sections 164.308 & 164.310	**We also offer Business Continuity Planning in accordance with HIPAA's guidelines.**

CONCLUSION: NOW IS THE TIME FOR A BACKUP SOLUTION THAT MEETS HIPAA STANDARDS

With the increasing enforcement of HIPAA regulators, the ease with which a Covered Entity can accidentally violate one of the law's many online-backup requirements, and the steep costs for making a mistake, your business should deploy an offsite backup solution to protect your ePHI as soon as possible.

Start by learning more about KeepItSafe's online backup and DR solutions—and how they can keep your business on the right side of HIPAA.

If you'd like to learn more about how KeepItSafe Online Backup can help your company reduce costs, save time, and stay compliant, contact one of our representatives today.

888 965 9988
info@keepitsafe.com